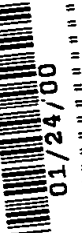


日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

10525 U.S. PTO
09/489696



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 3月 5日

出 願 番 号
Application Number:

平成11年特許願第059049号

願 人
Applicant(s):

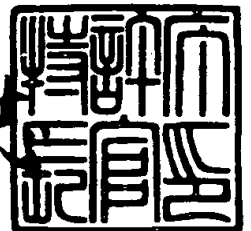
村田機械株式会社
辻井 重男
笠原 正雄

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 8月18日

特許庁長官
Commissioner,
Patent Office

伴佐山 建志



【書類名】 特許願

【整理番号】 20065

【提出日】 平成11年 3月 5日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/14
H04L 9/30
G09C 1/00

【発明の名称】 秘密鍵生成方法、暗号化方法及び暗号通信方法

【請求項の数】 3

【発明者】

【住所又は居所】 東京都渋谷区神宮前 4 - 2 - 1 9

【氏名】 辻井 重男

【発明者】

【住所又は居所】 大阪府箕面市栗生外院 4 丁目 1 5 番 3 号

【氏名】 笠原 正雄

【発明者】

【住所又は居所】 京都府京都市伏見区竹田向代町 1 3 6 番地 村田機械株式会社 本社工場内

【氏名】 村上 恭通

【特許出願人】

【識別番号】 000006297

【氏名又は名称】 村田機械株式会社

【代表者】 村田 純一

【特許出願人】

【住所又は居所】 東京都渋谷区神宮前 4 - 2 - 1 9

【氏名又は名称】 辻井 重男

【特許出願人】

【識別番号】 597008636

【氏名又は名称】 笠原 正雄

【代理人】

【識別番号】 100078868

【弁理士】

【氏名又は名称】 河野 登夫

【電話番号】 06-6944-4141

【手数料の表示】

【予納台帳番号】 001889

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9805283

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 秘密鍵生成方法、暗号化方法及び暗号通信方法

【特許請求の範囲】

【請求項 1】 エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、第 1 ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として前記秘密鍵を生成することを特徴とする秘密鍵生成方法。

【請求項 2】 各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、第 1 ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする暗号化方法。

【請求項 3】 センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、第 1 ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする暗号通信方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、エンティティ固有の秘密鍵を生成する秘密鍵生成方法、情報の内容が当事者以外にはわからないように情報を暗号化する暗号化方法、及び、暗号文にて通信を行う暗号通信方法に関する。

【0002】

【従来の技術】

高度情報化社会と呼ばれる現代社会では、コンピュータネットワークを基盤として、ビジネス上の重要な文書・画像情報が電子的な情報という形で伝送通信されて処理される。このような電子情報は、容易に複写が可能である、複写物とオリジナルとの区別が困難であるという性質があり、情報保全の問題が重要視されている。特に、「コンピュータリソースの共有」，「マルチアクセス」，「広域化」の各要素を満たすコンピュータネットワークの実現が高度情報化社会の確立に不可欠であるが、これは当事者間の情報保全の問題とは矛盾する要素を含んでいる。このような矛盾を解消するための有効な手法として、人類の過去の歴史上主として軍事、外交面で用いられてきた暗号技術が注目されている。

【0003】

暗号とは、情報の意味が当事者以外には理解できないように情報を交換することである。暗号において、誰でも理解できる元の文（平文）を第三者には意味がわからない文（暗号文）に変換することが暗号化であり、また、暗号文を平文に戻すことが復号であり、この暗号化と復号との全過程をまとめて暗号系と呼ぶ。暗号化の過程及び復号の過程には、それぞれ暗号化鍵及び復号鍵と呼ばれる秘密の情報が用いられる。復号時には秘密の復号鍵が必要であるので、この復号鍵を知っている者のみが暗号文を復号でき、暗号化によって情報の秘密性が維持され得る。

【0004】

暗号化鍵と復号鍵とは、等しくても良いし、異なっても良い。両者の鍵が等しい暗号方式は、共通鍵暗号方式と呼ばれ、米国商務省標準局が採用したDES (Data Encryption Standards)はその典型例である。このような共通鍵暗号方

式の従来例は、次のような3種の方法に分類できる。

【0005】

① 第1の方法

暗号通信を行う可能性がある相手との共通鍵をすべて秘密保管しておく方法

② 第2の方法

暗号通信の都度、予備通信により鍵を共有し合う方法（Diffie-Hellmanによる鍵共有方式、公開鍵方式による鍵配送方式など）。

③ 第3の方法

各ユーザ（エンティティ）の氏名、住所などの個人を特定する公開された特定情報（ID（Identity）情報）を利用して、予備通信を行うことなく、送信側のエンティティ、受信側のエンティティが独立に同一の共通鍵を生成する方法（KPS（Key Predistribution System）、ID-NIKS（ID-based Non-Interactive Key Sharing Schemes）など）。

【0006】

【発明が解決しようとする課題】

このような従来の3種の方法には、以下に述べるような問題がある。第1の方法では、すべての共通鍵を保管しておくようにするので、不特定多数のユーザがエンティティとなって暗号通信を行うネットワーク社会には適さない。また、第2の方法は、鍵共有のための予備通信が必要である点が問題である。

【0007】

第3の方法は、予備通信が不要であり、公開された相手のID情報とセンタから予め配布されている固有の秘密パラメータとを用いて、任意の相手との共通鍵を生成できるので、便利な方法である。しかしながら、次のような2つの問題点がある。一つは、センタがBig Brotherとなる（すべてのエンティティの秘密を握っており、Key Escrow Systemになってしまう）点である。もう一つは、ある数のエンティティが結託するとセンタの秘密を演算できる可能性がある点である。この結託問題については、これを計算量的に回避するための工夫が多数なされているが、完全な解決は困難である。

【0008】

この結託問題の難しさは、ID情報に基づく秘密パラメータがセンタ秘密と個人秘密との二重構造になっていることに起因する。第3の方法では、センタの公開パラメータと個人の公開ID情報とこの2種類の秘密パラメータとにて暗号系が構成され、しかも各エンティティが各自に配布された個人秘密を見せ合ってもセンタ秘密が露呈されないようにする必要がある。よって、その暗号系の構築の実現には解決すべき課題が多い。

【0009】

そこで、本発明者等は、特定情報（ID情報）をいくつかに分割し、複数の各センタからその分割した特定情報に基づくすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えることができ、結託問題の回避を可能にし、その暗号系の構築が容易であるID-NIKSによる秘密鍵生成方法、暗号化方法及び暗号通信方法を提案している（特願平11-16257号）。

【0010】

結託問題を解決することを目的として提案されてきたエンティティの特定情報に基づく種々の暗号系が不成功となった理由は、エンティティの結託情報からセンタ秘密を割り出せないようにするための工夫を数学的構造に求め過ぎていたためである。数学的構造が複雑過ぎると、安全性を証明するための方法も困難となる。そこで、特願平11-16257号の提案方法では、エンティティの特定情報をいくつかに分割し、分割した各特定情報についてすべての秘密鍵をエンティティに配布することにより、数学的構造を最小限に抑えるようにする。この提案方法では、複数のセンタが設けられ、各センタはあるエンティティの分割した1つの特定情報に対応する秘密鍵を生成する。よって、すべてのエンティティの秘密を1つのセンタが握るようなことはなく、各センタがBig Brotherにならない。

【0011】

そして、本発明者等は、この提案方法の改良を研究してきた。特に、特定のエンティティの攻撃に必要なすべてのエンティティを買収し、買収したエンティティの秘密鍵のすべてを用いることにより、その特定のエンティティを攻撃するという乱数置換攻撃に強い改良方法を研究してきた。

【0012】

本発明は斯かる事情に鑑みてなされたものであり、上記提案方法を改良してより乱数置換攻撃に強くした秘密鍵生成方法、暗号化方法及び暗号通信方法を提供することを目的とする。

【0013】

【課題を解決するための手段】

請求項1に係る秘密鍵生成方法は、エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、第1ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として前記秘密鍵を生成することを特徴とする。

【0014】

請求項2に係る暗号化方法は、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、第1ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする。

【0015】

請求項3に係る暗号通信方法は、センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含

まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、第1ブロックの分割特定情報に対する秘密鍵を複層構造とし、残りのブロックの分割特定情報に対する秘密鍵を単層構造として各エンティティ固有の秘密鍵を生成することを特徴とする。

【0016】

本発明では、全ブロックすべての計算を完了して初めて共通鍵が求められるようにしており、特定のエンティティの特定情報の分割ブロックを独立して攻撃できないようになっていて、乱数置換攻撃を回避できる。

【0017】

【発明の実施の形態】

以下、本発明の実施の形態について具体的に説明する。

図1は、本発明の暗号通信システムの構成を示す模式図である。情報の隠匿を信頼できる複数（K個）のセンタ1が設定されており、これらのセンタ1としては、例えば社会の公的機関を該当できる。

【0018】

これらの各センタ1と、この暗号系システムを利用するユーザとしての複数の各エンティティ a, b, \dots, z とは、秘密通信路 $2_{a1}, \dots, 2_{aK}, 2_{b1}, \dots, 2_{bK}, \dots, 2_{z1}, \dots, 2_{zK}$ により接続されており、これらの秘密通信路を介して各センタ1から秘密の鍵情報が各エンティティ a, b, \dots, z へ伝送されるようになっている。また、2人のエンティティの間には通信路 $3_{ab}, 3_{az}, 3_{bz}, \dots$ が設けられており、この通信路 $3_{ab}, 3_{az}, 3_{bz}, \dots$ を介して通信情報を暗号化した暗号文が互いのエンティティ間で伝送されるようになっている。

【0019】

（センタ1での準備処理）

センタ1は以下の公開鍵及び秘密鍵を準備し、公開鍵を公開する。

公開鍵 N $N = P Q$

K IDベクトルの分割ブロック数

M_j 分割したIDベクトルのサイズ（ $j = 1, 2, \dots, K$ ）

L IDベクトルのサイズ（ $L = M_1 + M_2 + \dots + M_K$ ）

T 指数部分の次数

秘密鍵 P, Q 大きな素数

g Nを法とする最大生成元

H_j 乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列

α_i エンティティ i の個人秘密乱数

(但し、 $\gcd(\alpha_i, \lambda(N)) = 1$,

$\lambda(\cdot)$ はカーマイケル関数)

β_{ij} エンティティ i の個人秘密乱数

(但し、 $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

【0020】

各エンティティの氏名、住所などを示す特定情報である ID ベクトルを L 次元 2 進ベクトルとし、図 2 に示すようにその ID ベクトルをブロックサイズ M_1 , M_2 , \dots , M_K 毎に K 個のブロックに分割する。例えば、エンティティ i の ID ベクトル (ベクトル I_i) を式 (1) のように分割する。分割特定情報である各ベクトル I_{ij} ($j = 1, 2, \dots, K$) を ID 分割ベクトルと呼ぶ。

【0021】

【数 1】

$$\overrightarrow{I_i} = [\overrightarrow{I_{i1}} | \overrightarrow{I_{i2}} | \dots | \overrightarrow{I_{iK}}] \quad \dots (1)$$

【0022】

(エンティティの登録処理)

エンティティ i に登録を依頼された各センタ 1 は、準備した鍵とエンティティ i の K 個の ID 分割ベクトルについて、それぞれに対応する K 個の秘密鍵ベクトル s_{ij} ($j = 1, 2, \dots, K$) を以下の式 (2-1), (2-2), \dots , (2-j), \dots , (2-K) に従って計算する。

【0023】

【数 2】

$$\overrightarrow{s_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1} \quad \dots (2-1)$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1} \quad \dots (2-2)$$

\vdots

$$\overrightarrow{s_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1} \quad \dots (2-j)$$

\vdots

$$\overrightarrow{s_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1} \quad \dots (2-K)$$

【0 0 2 4】

但し、ベクトル $\overrightarrow{1}$ は、すべての成分が 1 である K 次元のベクトルを表す。また、 H_j [ベクトル $\overrightarrow{I_{ij}}$] は対称行列 H_j からベクトル $\overrightarrow{I_{ij}}$ に対応した行を 1 行抜き出したものを表し、 $[\cdot]$ の操作を参照と定義する。

【0 0 2 5】

次に、第 1 ブロックに関して、 $(T+1)$ 個の秘密鍵ベクトル g_{it} ($t=0, 1, 2, \dots, T$) を以下の式 (3-0), (3-1), (3-2), \dots , (3-t), \dots , (3-T) に従って計算する。

【0 0 2 6】

【数3】

$$\begin{aligned}
 \overrightarrow{g_{i0}} &\equiv g^{\alpha_i^{-T} \overrightarrow{1}} \pmod{N} && \dots (3-0) \\
 \overrightarrow{g_{i1}} &\equiv g^{\alpha_i^{-T} \overrightarrow{s_{i1}}} \pmod{N} && \dots (3-1) \\
 \overrightarrow{g_{i2}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^2} \pmod{N} && \dots (3-2) \\
 &\vdots && \\
 \overrightarrow{g_{it}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^t} \pmod{N} && \dots (3-t) \\
 &\vdots && \\
 \overrightarrow{g_{iT}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^T} \pmod{N} && \dots (3-T)
 \end{aligned}$$

【0027】

但し、 c をスカラー、(4)、(5) に示す A 、 B を行列とした場合、 $B = c^A$ 及び $B = \langle A \rangle^c$ は、それぞれ (6) 及び (7) を表す。

【0028】

【数4】

$$A = (a_{\mu\nu}) \quad \dots (4)$$

$$B = (b_{\mu\nu}) \quad \dots (5)$$

$$b_{\mu\nu} = c^{a_{\mu\nu}} \quad \dots (6)$$

$$b_{\mu\nu} = a_{\mu\nu}^c \quad \dots (7)$$

【0029】

そして、1つのセンタ1は、第1ブロックに関する $(T+1)$ 個の秘密鍵ベクトル $\overrightarrow{g_{it}}$ ($t=0, 1, 2, \dots, T$) を秘密裏にエンティティ i へ送り、残りの $(K-1)$ の各センタ1は、第2ブロック以降に関する $(K-1)$ 個の秘密鍵ベクトル s_{ij} ($j=2, 3, \dots, K$) を秘密裏にエンティティ i へ送る。

【0 0 3 0】

(エンティティ間の共通鍵の生成処理)

エンティティ i は、第 1 ブロックに関して、自身の $(T+1)$ 個の秘密鍵ベクトル g_{it} の中から、エンティティ m の ID 分割ベクトルであるベクトル I_{m1} に対応する成分のベクトル g_{it} [ベクトル I_{m1}] を選び出す。この選び出したものを $(8-0)$, $(8-1)$, \dots , $(8-t)$, \dots , $(8-T)$ に示す。

【0 0 3 1】

【数 5】

$$\begin{aligned} g_{0im} &= \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] && \dots (8-0) \\ g_{1im} &= \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] && \dots (8-1) \\ &\vdots && \\ g_{tim} &= \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] && \dots (8-t) \\ &\vdots && \\ g_{Tim} &= \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}] && \dots (8-T) \end{aligned}$$

【0 0 3 2】

次に、エンティティ i は、 $j = 2, 3, \dots, K$ の第 2, 第 3, \dots , 第 K の各ブロックに関して、自身の秘密鍵ベクトル s_{ij} の中から、エンティティ m の ID 分割ベクトルであるベクトル I_{mj} に対応する成分のベクトル s_{ij} [ベクトル I_{mj}] を各ブロック毎に選び出す。この選び出したものを $(9-2)$, \dots , $(9-j)$, \dots , $(9-K)$ に示す。

【0 0 3 3】

【数 6】

$$\begin{aligned} x_{2im} &= \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}] && \dots (9-2) \\ &\vdots \\ x_{jim} &= \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}] && \dots (9-1) \\ &\vdots \\ x_{kim} &= \overrightarrow{s_{ik}}[\overrightarrow{I_{mk}}] && \dots (9-K) \end{aligned}$$

【0 0 3 4】

更に、(10) のように整数環上でこれらのすべての和 y_{im} を求める。

【0 0 3 5】

【数 7】

$$y_{im} = \sum_{j=2}^K x_{jim} \quad \dots (10)$$

【0 0 3 6】

そして、 N を法として以下の (11) のような計算を行うことにより、共通鍵 K_{im} を求める。この (11) の計算において、全ブロックの計算を完了することにより、個人秘密乱数 α_i はその逆元との乗算にて消去され、 K 個の個人秘密乱数 β_{ij} はそれらの加算にて消去される。この K_{im} はエンティティ m 側から求めた共通鍵 K_{mi} と一致する。

【0 0 3 7】

【数 8】

$$\begin{aligned}
K_{im} &\equiv \prod_{t=0}^T g_{tim}^T C_t y_{im}^{(T-t)} \\
&\equiv g_i^{\alpha_i^{-T}} \sum_{t=0}^T C_t x_{tim}^t y_{im}^{T-t} \\
&\equiv g_i^{\alpha_i^{-T}} (x_{im} + y_{im})^T \\
&\equiv g_i^{\alpha_i^{-T}} (x_{im} + \dots + x_{kim})^T \\
&\equiv g_i^{\alpha_i^{-T}} (\alpha_i H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \beta_{i1} + \dots + \alpha_i H_K [\vec{I}_{iK}] [\vec{I}_{mK}] + \beta_{iK})^T \\
&\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}]) + \lambda(N) \}^T \\
&\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1 [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}]) \}^T \\
&\equiv g^{(H_i [\vec{I}_{i1}] [\vec{I}_{m1}] + \dots + H_K [\vec{I}_{iK}] [\vec{I}_{mK}])^T} \pmod{N} \\
&\dots (11)
\end{aligned}$$

【0038】

なお、上式において $x_{im} =$ ベクトル s_{i1} [ベクトル I_{m1}] と置いたが、これは、エンティティ i 自身にもわからない。また、 T は比較的小さな数であるので、指数部分はべき乗を順次繰り返し行うことにより計算することができる。

【0039】

なお、上記例において、各ブロックのサイズ M_j は全ブロックにおいて一定であっても良いし、その一部または全部のブロックで異なっても良い。しかし、第1ブロックに関して秘密鍵ベクトル g_{it} を求めるので、全ブロックについてそのサイズを一定にした場合、第1ブロックについての秘密が大きくなってしまふ。よって、第1ブロックのサイズを他のブロックのサイズよりも小さくするようにした方が良い。特に、 $M_1 = 1$ とした場合、配布する秘密を最小限にすることができ、最も安全性が高くなる。

【0040】

ここで、不特定多数のエンティティの結託によって暗号システム全体を攻撃するような結託攻撃に対する本発明の安全性について考察する。エンティティの総数を100万人とした場合、 $1000000 \approx 2^{20}$ であるので、 $M_j = 1$ 、 $K=20$ となる。ここで、 $T=32$ とした場合、共有鍵 K_{im} の指数部分の項数は、 ${}_{20}H_{32} = {}_{51}C_{32} \approx 4.85 \times 10^{13}$ となる。この項数は、全エンティティ間の共有鍵の総数 ${}_{1000000}C_2 \approx 5 \times 10^{12}$ を超える。よって、項数>共有鍵の総数の条件を満たし、結託攻撃に対して安全である。

【0041】

次に、上述した暗号システムにおけるエンティティ間の情報の通信について説明する。図3は、2人のエンティティ a, b 間における情報の通信状態を示す模式図である。図3の例は、エンティティ a が平文（メッセージ）Mを暗号文Cに暗号化してそれをエンティティ b へ伝送し、エンティティ b がその暗号文Cを元の平文（メッセージ）Mに復号する場合を示している。

【0042】

1番目のセンタ1には、各エンティティ a, b 固有の秘密鍵ベクトル s_{a1} , s_{b1} と $(T+1)$ 個の秘密鍵ベクトル g_{at} , g_{bt} ($t=0, 1, 2, \dots, T$) とを、前記式 (2-1) と (3-0), \dots , (3-T) とに従って計算する秘密鍵生成器 1a が備えられている。そして、各エンティティ a, b から登録が依頼されると、そのエンティティ a, b の秘密鍵ベクトル g_{at} , g_{bt} がエンティティ a, b へ送付される。

【0043】

j ($j=2, 3, \dots, K$) 番目のセンタ1には、各エンティティ a, b 固有の秘密鍵ベクトル s_{aj} , s_{bj} を前記式 (2-2), \dots , (2-K) に従って計算する秘密鍵生成器 1a が備えられている。そして、各エンティティ a, b から登録が依頼されると、そのエンティティ a, b の秘密鍵ベクトル s_{aj} , s_{bj} がエンティティ a, b へ送付される。

【0044】

エンティティ a 側には、各センタ1から送られるこれらの秘密鍵ベクトル g_{at}

($t = 0, 1, 2, \dots, T$), s_{aj} ($j = 2, 3, \dots, K$) をテーブル形式で格納しているメモリ 10 と、これらの秘密鍵ベクトルの中からエンティティ b に対応する成分であるベクトル g_{at} [ベクトル I_{b1}] ($t = 0, 1, 2, \dots, T$), ベクトル s_{aj} [ベクトル I_{bj}] ($j = 2, 3, \dots, K$) を選び出す成分選出器 11 と、選び出されたこれらの成分を使用してエンティティ a が求めるエンティティ b との共通鍵 K_{ab} を生成する共通鍵生成器 12 と、共通鍵 K_{ab} を用いて平文 (メッセージ) M を暗号文 C に暗号化して通信路 30 へ出力する暗号化器 13 とが備えられている。

【0045】

また、エンティティ b 側には、各センタ 1 から送られるこれらの秘密鍵ベクトル g_{bt} ($t = 0, 1, 2, \dots, T$), s_{bj} ($j = 2, 3, \dots, K$), をテーブル形式で格納しているメモリ 20 と、これらの秘密ベクトルの中からエンティティ a に対応する成分であるベクトル g_{bt} [ベクトル I_{a1}] ($t = 0, 1, 2, \dots, T$), ベクトル s_{bj} [ベクトル I_{aj}] ($j = 2, 3, \dots, K$) を選び出す成分選出器 21 と、選び出されたこれらの成分を使用してエンティティ b が求めるエンティティ a との共通鍵 K_{ba} を生成する共通鍵生成器 22 と、共通鍵 K_{ba} を用いて通信路 30 から入力した暗号文 C を平文 M に復号して出力する復号器 23 とが備えられている。

【0046】

エンティティ a からエンティティ b へ情報を伝送しようとする場合、まず、各センタ 1 で求められて、予めメモリ 10 に格納されている秘密鍵ベクトル g_{at} ($t = 0, 1, 2, \dots, T$), s_{aj} ($j = 2, 3, \dots, K$) が成分選出器 11 へ読み出される。そして、成分選出器 11 にて、エンティティ b に対応する成分であるベクトル g_{at} [ベクトル I_{b1}] ($t = 0, 1, 2, \dots, T$), ベクトル s_{aj} [ベクトル I_{bj}] ($j = 2, 3, \dots, K$) が選び出されて共通鍵生成器 12 へ送られる。共通鍵生成器 12 にて、これらの成分を使用して (11) に従って共通鍵 K_{ab} が求められ、暗号化器 13 へ送られる。暗号化器 13 において、この共通鍵 K_{ab} を用いて平文 M が暗号文 C に暗号化され、暗号文 C が通信路 30 を介して伝送される。

【0047】

通信路 30 を伝送された暗号文 C はエンティティ b の復号器 23 へ入力される。各センタ 1 で求められて、予めメモリ 20 に格納されている秘密鍵ベクトル s_{bj} ($j = 2, 3, \dots, K$), g_{bt} ($t = 0, 1, 2, \dots, T$) が成分選出器 21 へ読み出される。そして、成分選出器 21 にて、エンティティ a に対応する成分であるベクトル g_{bt} [ベクトル I_{a1}] ($t = 0, 1, 2, \dots, T$), ベクトル s_{bj} [ベクトル I_{aj}] ($j = 2, 3, \dots, K$) が選出されて共通鍵生成器 22 へ送られる。共通鍵生成器 22 にて、これらの成分を使用して (11) に従って共通鍵 K_{ba} が求められ、復号器 23 へ送られる。復号器 23 において、この共通鍵 K_{ba} を用いて暗号文 C が平文 M に復号される。

【0048】

このような例では、複数のセンタが設けられ、各センタはエンティティの分割した 1 つの ID 情報に対応する鍵を生成するようにしたので、すべてのエンティティの秘密を 1 つのセンタが握るようなことはなく、各センタが Big Brother にならない。また、各エンティティ固有の秘密鍵ベクトルが予めエンティティ側のメモリに格納されているので、共通鍵生成に要する時間が短くて済む。

【0049】

図 4 は、本発明の記録媒体の実施の形態の構成を示す図である。ここに例示するプログラムは、各センタからエンティティ i へ送られてくる秘密鍵ベクトル s_{ij} , g_{it} の中からエンティティ m に対応する成分を選び出す処理と、これらの選出成分を使用して共通鍵 K_{im} を求める処理とを含んでおり、以下に説明する記録媒体に記録されている。なお、コンピュータ 40 は、各エンティティ側に設けられている。

【0050】

図 4 において、コンピュータ 40 とオンライン接続する記録媒体 41 は、コンピュータ 40 の設置場所から隔たって設置される例えば WWW (World Wide Web) のサーバコンピュータを用いてなり、記録媒体 41 には前述の如きプログラム 41a が記録されている。記録媒体 41 から読み出されたプログラム 41a がコンピュータ 40 を制御することにより、各エンティティにおいて通信対象のエンテ

ィティに対する共通鍵を演算する。

【0051】

コンピュータ40の内部に設けられた記録媒体42は、内蔵設置される例えばハードディスクドライブまたはROMなどを用いてなり、記録媒体42には前述の如きプログラム42aが記録されている。記録媒体42から読み出されたプログラム42aがコンピュータ40を制御することにより、各エンティティにおいて通信対象のエンティティに対する共通鍵を演算する。

【0052】

コンピュータ40に設けられたディスクドライブ40aに装填して使用される記録媒体43は、運搬可能な例えば光磁気ディスク、CD-ROMまたはフレキシブルディスクなどを用いてなり、記録媒体43には前述の如きプログラム43aが記録されている。記録媒体43から読み出されたプログラム43aがコンピュータ40を制御することにより、各エンティティにおいて通信対象のエンティティに対する共通鍵を演算する。

【0053】

【発明の効果】

以上詳述したように、本発明では、全ブロックすべての計算を完了して初めて乱数項が消去されるようにしているので、分割ブロックを独立して攻撃できないようになっていて、乱数置換攻撃を回避することが可能である。

【0054】

(付記)

なお、以上の説明に対して更に以下の項を開示する。

(1) エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して、前記エンティティ固有の秘密鍵を生成する方法において、前記秘密鍵を生成する演算式は以下である秘密鍵生成方法。

【0055】

【数 9】

$$\vec{s}_{i1} = \alpha_i H_1 [\vec{I}_{i1}] + \beta_{i1} \vec{1}$$

$$\vec{s}_{i2} = \alpha_i H_2 [\vec{I}_{i2}] + \beta_{i2} \vec{1}$$

⋮

$$\vec{s}_{ij} = \alpha_i H_j [\vec{I}_{ij}] + \beta_{ij} \vec{1}$$

⋮

$$\vec{s}_{iK} = \alpha_i H_K [\vec{I}_{iK}] + \beta_{iK} \vec{1}$$

$$\vec{g}_{i0} \equiv g^{\alpha_i^{-T} \vec{1}} \pmod{N}$$

$$\vec{g}_{i1} \equiv g^{\alpha_i^{-T} \vec{s}_{i1}} \pmod{N}$$

$$\vec{g}_{i2} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^2} \pmod{N}$$

⋮

$$\vec{g}_{it} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^t} \pmod{N}$$

⋮

$$\vec{g}_{iT} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^T} \pmod{N}$$

【0056】

但し、

ベクトル s_{ij} : エンティティ i の j 番目の分割特定情報に対応する秘

密鍵 ($j = 1, 2, \dots, K$)

[ベクトル I_{ij}] : エンティティ i の j 番目の分割特定情報

ベクトル 1 : 成分がすべて 1 である K 次元ベクトル

H_j : 乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列

M_j : エンティティ i の j 番目の分割特定情報のサイズ

K : エンティティ i の特定情報のブロック分割数

α_i : エンティティ i の個人秘密乱数

(但し、 $\gcd(\alpha_i, \lambda(N)) = 1$,

$\lambda(\cdot)$ はカーマイケル関数)

N : $N = PQ$ (P, Q は素数)

β_{ij} : エンティティ i の個人秘密乱数

(但し、 $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

g : N を法とする最大生成元

ベクトル g_{it} : エンティティ i の特定情報の第 1 ブロックに関する秘密鍵 ($t = 0, 1, 2, \dots, T$)

T : 指数部分の次数

c をスカラーとし、(i), (ii) に示す A, B を行列した場合、 $B = c^A$ 及び $B = \langle A \rangle^c$ は、それぞれ (iii) 及び (iv) を表す

【0057】

【数10】

$$A = (a_{\mu\nu}) \quad \dots (i)$$

$$B = (b_{\mu\nu}) \quad \dots (ii)$$

$$b_{\mu\nu} = c^{a_{\mu\nu}} \quad \dots (iii)$$

$$b_{\mu\nu} = a_{\mu\nu}^c \quad \dots (iv)$$

【0058】

(2) 各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、この秘密鍵に含まれている、暗号文の送信先である相手のエンティティの分割特定情報に対応する成分を使用して生成した共通鍵を用いて平文を暗号文に暗号化する暗号化方法において、各エンティティ固有の秘密鍵を生成する演算式は以下である暗号化方法。

【0059】

【数 11】

$$\overrightarrow{s_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

⋮

$$\overrightarrow{s_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$

⋮

$$\overrightarrow{s_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T} \overrightarrow{1}} \pmod{N}$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T} \overrightarrow{s_{i1}}} \pmod{N}$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^2} \pmod{N}$$

⋮

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^t} \pmod{N}$$

⋮

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^T} \pmod{N}$$

【0060】

但し、

ベクトル s_{ij} : エンティティ i の j 番目の分割特定情報に対応する秘

密鍵 ($j = 1, 2, \dots, K$)

[ベクトル I_{ij}] : エンティティ i の j 番目の分割特定情報

ベクトル 1 : 成分がすべて 1 である K 次元ベクトル

H_j : 乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列

M_j : エンティティ i の j 番目の分割特定情報のサイズ

K : エンティティ i の特定情報のブロック分割数

α_i : エンティティ i の個人秘密乱数

(但し、 $\gcd(\alpha_i, \lambda(N)) = 1$,

$\lambda(\cdot)$ はカーマイケル関数)

N : $N = PQ$ (P, Q は素数)

β_{ij} : エンティティ i の個人秘密乱数

(但し、 $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

g : N を法とする最大生成元

ベクトル g_{it} : エンティティ i の特定情報の第 1 ブロックに関する秘密鍵 ($t = 0, 1, 2, \dots, T$)

T : 指数部分の次数

c をスカラーとし、(i), (ii) に示す A, B を行列した場合、 $B = c^A$ 及び $B = \langle A \rangle^c$ は、それぞれ (iii) 及び (iv) を表す

【0061】

【数 12】

$$A = (a_{\mu\nu}) \quad \dots (i)$$

$$B = (b_{\mu\nu}) \quad \dots (ii)$$

$$b_{\mu\nu} = c^{a_{\mu\nu}} \quad \dots (iii)$$

$$b_{\mu\nu} = a_{\mu\nu}^c \quad \dots (iv)$$

【0062】

(3) 第(2)項記載の暗号化方法であって、前記共通鍵を生成する演算式は以下である暗号化方法。

【0063】

【数 13】

$$\begin{aligned}
 g_{0im} &= \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}] \\
 g_{1im} &= \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}] \\
 &\vdots \\
 g_{tim} &= \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}] \\
 &\vdots \\
 g_{Tim} &= \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}] \\
 x_{2im} &= \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}] \\
 &\vdots \\
 x_{jim} &= \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}] \\
 &\vdots \\
 x_{kim} &= \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]
 \end{aligned}$$

$$\begin{aligned}
 K_{im} &\equiv \prod_{t=0}^T g_{tim}^T C_t y_{im}^{(T-t)} \\
 &\equiv g_i^{\alpha_i^{-T}} \sum_{t=0}^T \overrightarrow{C_t} x_{tim}^t y_{im}^{T-t} \\
 &\equiv g_i^{\alpha_i^{-T}} (x_{1im} + y_{im})^T \\
 &\equiv g_i^{\alpha_i^{-T}} (x_{1im} + \dots + x_{kim})^T \\
 &\equiv g_i^{\alpha_i^{-T}} (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}] + \beta_{iK})^T \\
 &\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) + \lambda(N) \}^T \\
 &\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) \}^T \\
 &\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \pmod{N}
 \end{aligned}$$

【0064】

但し、

g_{tim} (=ベクトル g_{it} [ベクトル I_{m1}])

: エンティティ i の特定情報の第 1 ブロックについて自身のベクトル g_{it} から選び出した、エンティティ m のベクトル I_{m1} に対応する成分 ($t = 0, 1, 2, \dots, T$)

x_{1im} = ベクトル s_{i1} [ベクトル I_{m1}]

x_{jim} (=ベクトル s_{ij} [ベクトル I_{mj}])

: エンティティ i の特定情報の第 j ブロックについて自身のベクトル s_{ij} から選び出した、エンティティ m のベクトル I_{mj} に対応する成分 ($j = 2, 3, \dots, K$)

K_{im} : 一方のエンティティ i が他方のエンティティ m に対して生成する共通鍵

y_{im} : $(K-1)$ 個の x_{jim} の和 ($j = 2, 3, \dots, K$)

即ち、 $y_{im} = x_{2im} + x_{3im} + \dots + x_{Kim}$

【0065】

(4) センタから各エンティティへ各エンティティ固有の秘密鍵を送付し、一方のエンティティが前記センタから送付された該エンティティ固有の秘密鍵から求めた共通鍵を用いて平文を暗号文に暗号化して他方のエンティティへ伝送し、該他方のエンティティが伝送された暗号文を、前記センタから送付された該エンティティ固有の秘密鍵から求めた、前記共通鍵と同一の共通鍵を用いて元の平文に復号することにより、エンティティ間で情報の通信を行うこととし、前記センタが複数設けられており、その複数の各センタは、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して各エンティティ固有の秘密鍵を生成し、各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して前記共通鍵を生成するようにした暗号通信方法において、前記センタにおける秘密鍵を生成する演算式は以下である暗号通信方法。

【0066】

【数 14】

$$\begin{aligned}
 \overrightarrow{s_{i1}} &= \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1} \\
 \overrightarrow{s_{i2}} &= \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1} \\
 &\vdots \\
 \overrightarrow{s_{ij}} &= \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1} \\
 &\vdots \\
 \overrightarrow{s_{iK}} &= \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1} \\
 \\
 \overrightarrow{g_{i0}} &\equiv g^{\alpha_i^{-T} \overrightarrow{1}} \pmod{N} \\
 \overrightarrow{g_{i1}} &\equiv g^{\alpha_i^{-T} \overrightarrow{s_{i1}}} \pmod{N} \\
 \overrightarrow{g_{i2}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^2} \pmod{N} \\
 &\vdots \\
 \overrightarrow{g_{it}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^t} \pmod{N} \\
 &\vdots \\
 \overrightarrow{g_{iT}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^T} \pmod{N}
 \end{aligned}$$

【0067】

但し、

ベクトル s_{ij} : エンティティ i の j 番目の分割特定情報に対応する秘密鍵 ($j = 1, 2, \dots, K$)

[ベクトル I_{ij}] : エンティティ i の j 番目の分割特定情報

ベクトル 1 : 成分がすべて 1 である K 次元ベクトル

H_j : 乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列

M_j : エンティティ i の j 番目の分割特定情報のサイズ

K : エンティティ i の特定情報のブロック分割数

α_i : エンティティ i の個人秘密乱数

(但し、 $\gcd(\alpha_i, \lambda(N)) = 1$,

$\lambda(\cdot)$ はカーマイケル関数)

N : $N = PQ$ (P, Q は素数)

β_{ij} : エンティティ i の個人秘密乱数

(但し、 $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

g : N を法とする最大生成元

ベクトル g_{it} : エンティティ i の特定情報の第 1 ブロックに関する秘密鍵 ($t = 0, 1, 2, \dots, T$)

T : 指数部分の次数

c をスカラーとし、(i), (ii) に示す A, B を行列した場合、 $B = c^A$ 及び $B = \langle A \rangle^c$ は、それぞれ (iii) 及び (iv) を表す

【0068】

【数15】

$$A = (a_{\mu\nu}) \quad \dots (i)$$

$$B = (b_{\mu\nu}) \quad \dots (ii)$$

$$b_{\mu\nu} = c^{a_{\mu\nu}} \quad \dots (iii)$$

$$b_{\mu\nu} = a_{\mu\nu}^c \quad \dots (iv)$$

【0069】

(5) 第(4)項記載の暗号通信方法であって、前記共通鍵を生成する演算式は以下である暗号通信方法。

【0070】

【数 16】

$$g_{0im} = \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$

$$\vdots$$

$$x_{kim} = \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]$$

$$K_{im} \equiv \prod_{t=0}^T g_{tim}^T C_t y_{im}^{(T-t)}$$

$$\equiv g^{\alpha_i^{-T}} \sum_{t=0}^T C_t x_{im}^t y_{im}^{T-t}$$

$$\equiv g^{\alpha_i^{-T}} (x_{im} + y_{im})^T$$

$$\equiv g^{\alpha_i^{-T}} (x_{im} + \dots + x_{kim})^T$$

$$\equiv g^{\alpha_i^{-T}} (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}] + \beta_{iK})^T$$

$$\equiv g^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) + \lambda(N) \}^T$$

$$\equiv g^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) \}^T$$

$$\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \pmod{N}$$

【0071】

但し、

g_{tim} (=ベクトル g_{it} [ベクトル I_{m1}])

: エンティティ i の特定情報の第 1 ブロックについて自身のベクトル g_{it} から選び出した、エンティティ m のベクトル I_{m1} に対応する成分 ($t = 0, 1, 2, \dots, T$)

$x_{1im} =$ ベクトル s_{i1} [ベクトル I_{m1}]

x_{jim} (=ベクトル s_{ij} [ベクトル I_{mj}])

: エンティティ i の特定情報の第 j ブロックについて自身のベクトル s_{ij} から選び出した、エンティティ m のベクトル I_{mj} に対応する成分 ($j = 2, 3, \dots, K$)

K_{im} : 一方のエンティティ i が他方のエンティティ m に対して生成する共通鍵

y_{im} : $(K-1)$ 個の x_{jim} の和 ($j = 2, 3, \dots, K$)

即ち、 $y_{im} = x_{2im} + x_{3im} + \dots + x_{Kim}$

【0072】

(6) 暗号通信システムのエンティティに設けられており、平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵を生成する共通鍵生成装置において、前記エンティティの特定情報を複数のブロックに分割した分割特定情報毎に以下の演算式に従って作成された前記エンティティ固有の秘密鍵を格納する格納手段と、格納されている秘密鍵の中から、通信相手のエンティティの分割特定情報に対応する成分を選び出す選出手段と、選び出した成分を使用して以下の演算式に従って前記共通鍵を生成する手段とを備える共通鍵生成装置。

【0073】

【数 17】

$$\begin{aligned}
 \overrightarrow{s_{i1}} &= \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1} \\
 \overrightarrow{s_{i2}} &= \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1} \\
 &\vdots \\
 \overrightarrow{s_{ij}} &= \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1} \\
 &\vdots \\
 \overrightarrow{s_{iK}} &= \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1} \\
 \\
 \overrightarrow{g_{i0}} &\equiv g^{\alpha_i^{-T} \overrightarrow{1}} \pmod{N} \\
 \overrightarrow{g_{i1}} &\equiv g^{\alpha_i^{-T} \overrightarrow{s_{i1}}} \pmod{N} \\
 \overrightarrow{g_{i2}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^2} \pmod{N} \\
 &\vdots \\
 \overrightarrow{g_{it}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^t} \pmod{N} \\
 &\vdots \\
 \overrightarrow{g_{iT}} &\equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^T} \pmod{N}
 \end{aligned}$$

【0074】

但し、

ベクトル s_{ij} : エンティティ i の j 番目の分割特定情報に対応する秘

密鍵 ($j = 1, 2, \dots, K$)

[ベクトル I_{ij}] : エンティティ i の j 番目の分割特定情報

ベクトル 1 : 成分がすべて 1 である K 次元ベクトル

H_j : 乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列

M_j : エンティティ i の j 番目の分割特定情報のサイズ

K : エンティティ i の特定情報のブロック分割数

α_i : エンティティ i の個人秘密乱数

(但し、 $\gcd(\alpha_i, \lambda(N)) = 1$,

$\lambda(\cdot)$ はカーマイケル関数)

$N : N = PQ$ (P, Q は素数)

β_{ij} : エンティティ i の個人秘密乱数

(但し、 $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

g : N を法とする最大生成元

ベクトル g_{it} : エンティティ i の特定情報の第 1 ブロックに関する秘密鍵 ($t = 0, 1, 2, \dots, T$)

T : 指数部分の次数

c をスカラーとし、(i), (ii) に示す A, B を行列した場合、 $B = c^A$ 及び $B = \langle A \rangle^c$ は、それぞれ (iii) 及び (iv) を表す

【0075】

【数18】

$$A = (a_{\mu\nu}) \dots (i)$$

$$B = (b_{\mu\nu}) \dots (ii)$$

$$b_{\mu\nu} = c^{a_{\mu\nu}} \dots (iii)$$

$$b_{\mu\nu} = a_{\mu\nu}^c \dots (iv)$$

【0076】

【数 19】

$$g_{0im} = \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$

$$\vdots$$

$$x_{kim} = \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]$$

$$K_{im} \equiv \prod_{t=0}^T g_{tim}^T C_t y_{im}^{(T-t)}$$

$$\equiv g_i^{\alpha_i^{-T}} \sum_{t=0}^T C_t x_{1im}^t y_{im}^{T-t}$$

$$\equiv g_i^{\alpha_i^{-T}} (x_{1im} + y_{im})^T$$

$$\equiv g_i^{\alpha_i^{-T}} (x_{1im} + \dots + x_{kim})^T$$

$$\equiv g_i^{\alpha_i^{-T}} (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}] + \beta_{iK})^T$$

$$\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) + \lambda(N) \}^T$$

$$\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) \}^T$$

$$\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \pmod{N}$$

【0077】

但し、

g_{tim} (=ベクトル g_{it} [ベクトル I_{m1}])

: エンティティ i の特定情報の第 1 ブロックについて自身のベクトル g_{it} から選び出した、エンティティ m のベクトル I_{m1} に対応する成分 ($t = 0, 1, 2, \dots, T$)

$x_{1im} =$ ベクトル s_{i1} [ベクトル I_{m1}]

x_{jim} (=ベクトル s_{ij} [ベクトル I_{mj}])

: エンティティ i の特定情報の第 j ブロックについて自身のベクトル s_{ij} から選び出した、エンティティ m のベクトル I_{mj} に対応する成分 ($j = 2, 3, \dots, K$)

K_{im} : 一方のエンティティ i が他方のエンティティ m に対して生成する共通鍵

y_{im} : ($K-1$) 個の x_{jim} の和 ($j = 2, 3, \dots, K$)

即ち、 $y_{im} = x_{2im} + x_{3im} + \dots + x_{Kim}$

【0078】

(7) 送信すべき情報である平文を暗号文に暗号化する暗号化処理、及び、送信された暗号文を元の平文に復号する復号処理を、複数のエンティティ間で相互に行う暗号通信システムにおいて、各エンティティの特定情報を複数のブロックに分割した分割特定情報を利用して以下の演算式に従い各エンティティ固有の秘密鍵を生成して各エンティティへ送付する複数のセンタと、該センタから送付された自身の秘密鍵に含まれている、通信対象のエンティティの分割特定情報に対応する成分を使用して以下の演算式に従い、前記暗号化処理及び復号処理に用いる共通鍵を生成する複数のエンティティとを有する暗号通信システム。

【0079】

【数 20】

$$\vec{s}_{i1} = \alpha_i H_1 [\vec{I}_{i1}] + \beta_{i1} \vec{1}$$

$$\vec{s}_{i2} = \alpha_i H_2 [\vec{I}_{i2}] + \beta_{i2} \vec{1}$$

⋮

$$\vec{s}_{ij} = \alpha_i H_j [\vec{I}_{ij}] + \beta_{ij} \vec{1}$$

⋮

$$\vec{s}_{iK} = \alpha_i H_K [\vec{I}_{iK}] + \beta_{iK} \vec{1}$$

$$\vec{g}_{i0} \equiv g^{\alpha_i^{-T} \vec{1}} \pmod{N}$$

$$\vec{g}_{i1} \equiv g^{\alpha_i^{-T} \vec{s}_{i1}} \pmod{N}$$

$$\vec{g}_{i2} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^2} \pmod{N}$$

⋮

$$\vec{g}_{it} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^t} \pmod{N}$$

⋮

$$\vec{g}_{iT} \equiv g^{\alpha_i^{-T} \langle \vec{s}_{i1} \rangle^T} \pmod{N}$$

【0080】

但し、

ベクトル s_{ij} : エンティティ i の j 番目の分割特定情報に対応する秘

密鍵 ($j = 1, 2, \dots, K$)

[ベクトル I_{ij}] : エンティティ i の j 番目の分割特定情報

ベクトル 1 : 成分がすべて 1 である K 次元ベクトル

H_j : 乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列

M_j : エンティティ i の j 番目の分割特定情報のサイズ

K : エンティティ i の特定情報のブロック分割数

α_i : エンティティ i の個人秘密乱数

(但し、 $\gcd(\alpha_i, \lambda(N)) = 1$,

$\lambda(\cdot)$ はカーマイケル関数)

N : $N = PQ$ (P, Q は素数)

β_{ij} : エンティティ i の個人秘密乱数

(但し、 $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

g : N を法とする最大生成元

ベクトル g_{it} : エンティティ i の特定情報の第 1 ブロックに関する秘密鍵 ($t = 0, 1, 2, \dots, T$)

T : 指数部分の次数

c をスカラーとし、(i), (ii) に示す A, B を行列した場合、 $B = c^A$ 及び $B = \langle A \rangle^c$ は、それぞれ (iii) 及び (iv) を表す

【0081】

【数 2 1】

$$\begin{aligned} A &= (a_{\mu\nu}) && \dots (i) \\ B &= (b_{\mu\nu}) && \dots (ii) \\ b_{\mu\nu} &= c^{a_{\mu\nu}} && \dots (iii) \\ b_{\mu\nu} &= a_{\mu\nu}^c && \dots (iv) \end{aligned}$$

【0082】

【数 2 2】

$$g_{0im} = \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$

$$\vdots$$

$$x_{kim} = \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]$$

$$K_{im} \equiv \prod_{t=0}^T g_{tim}^T C_t y_{im}^{(T-t)}$$

$$\equiv g_i^{\alpha_i^{-T}} \sum_{t=0}^T C_t x_{1im}^t y_{im}^{T-t}$$

$$\equiv g_i^{\alpha_i^{-T}} (x_{1im} + y_{im})^T$$

$$\equiv g_i^{\alpha_i^{-T}} (x_{1im} + \cdots + x_{kim})^T$$

$$\equiv g_i^{\alpha_i^{-T}} (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \beta_{i1} + \cdots + \alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}] + \beta_{iK})^T$$

$$\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) + \lambda(N) \}^T$$

$$\equiv g_i^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) \}^T$$

$$\equiv g_i^{\alpha_i^{-T}} (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \cdots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T \pmod{N}$$

【0083】

但し、

g_{tim} (=ベクトル g_{it} [ベクトル I_{m1}])

: エンティティ i の特定情報の第1ブロックについて自身のベクトル g_{it} から選び出した、エンティティ m のベクトル I_{m1} に対応する成分 ($t = 0, 1, 2, \dots, T$)

$x_{1im} =$ ベクトル s_{i1} [ベクトル I_{m1}]

x_{jim} (=ベクトル s_{ij} [ベクトル I_{mj}])

: エンティティ i の特定情報の第 j ブロックについて自身のベクトル s_{ij} から選び出した、エンティティ m のベクトル I_{mj} に対応する成分 ($j = 2, 3, \dots, K$)

K_{im} : 一方のエンティティ i が他方のエンティティ m に対して生成する共通鍵

y_{im} : ($K-1$) 個の x_{jim} の和 ($j = 2, 3, \dots, K$)

即ち、 $y_{im} = x_{2im} + x_{3im} + \dots + x_{Kim}$

【0084】

(8) 暗号通信システムにおける平文から暗号文への暗号化処理及び暗号文から平文への復号処理に用いる共通鍵をエンティティ側で生成するためのプログラムを記録してあるコンピュータでの読み取り可能な記録媒体において、前記エンティティの特定情報を複数のブロックに分割した分割特定情報毎に以下の演算式に従って作成された前記エンティティ固有の秘密鍵の中から、通信相手のエンティティの分割特定情報に対応する成分を選び出すことを前記コンピュータにさせるプログラムコード手段と、選び出した成分を使用して以下の演算式に従って前記共通鍵を生成することを前記コンピュータにさせるプログラムコード手段とを有する記録媒体。

【0085】

【数 2 3】

$$\overrightarrow{s_{i1}} = \alpha_i H_1 [\overrightarrow{I_{i1}}] + \beta_{i1} \overrightarrow{1}$$

$$\overrightarrow{s_{i2}} = \alpha_i H_2 [\overrightarrow{I_{i2}}] + \beta_{i2} \overrightarrow{1}$$

⋮

$$\overrightarrow{s_{ij}} = \alpha_i H_j [\overrightarrow{I_{ij}}] + \beta_{ij} \overrightarrow{1}$$

⋮

$$\overrightarrow{s_{iK}} = \alpha_i H_K [\overrightarrow{I_{iK}}] + \beta_{iK} \overrightarrow{1}$$

$$\overrightarrow{g_{i0}} \equiv g^{\alpha_i^{-T} \overrightarrow{1}} \pmod{N}$$

$$\overrightarrow{g_{i1}} \equiv g^{\alpha_i^{-T} \overrightarrow{s_{i1}}} \pmod{N}$$

$$\overrightarrow{g_{i2}} \equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^2} \pmod{N}$$

⋮

$$\overrightarrow{g_{it}} \equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^t} \pmod{N}$$

⋮

$$\overrightarrow{g_{iT}} \equiv g^{\alpha_i^{-T} \langle \overrightarrow{s_{i1}} \rangle^T} \pmod{N}$$

【0 0 8 6】

但し、

ベクトル s_{ij} : エンティティ i の j 番目の分割特定情報に対応する秘

密鍵 ($j = 1, 2, \dots, K$)

[ベクトル I_{ij}] : エンティティ i の j 番目の分割特定情報

ベクトル 1 : 成分がすべて 1 である K 次元ベクトル

H_j : 乱数からなる $2^{M_j} \times 2^{M_j}$ の対称行列

M_j : エンティティ i の j 番目の分割特定情報のサイズ

K : エンティティ i の特定情報のブロック分割数

α_i : エンティティ i の個人秘密乱数

(但し、 $\gcd(\alpha_i, \lambda(N)) = 1$,

$\lambda(\cdot)$ はカーマイケル関数)

N : $N = PQ$ (P, Q は素数)

β_{ij} : エンティティ i の個人秘密乱数

(但し、 $\beta_{i1} + \beta_{i2} + \dots + \beta_{iK} = \lambda(N)$)

g : N を法とする最大生成元

ベクトル g_{it} : エンティティ i の特定情報の第 1 ブロックに関する秘密鍵 ($t = 0, 1, 2, \dots, T$)

T : 指数部分の次数

c をスカラーとし、(i), (ii) に示す A, B を行列した場合、 $B = c^A$ 及び $B = \langle A \rangle^c$ は、それぞれ (iii) 及び (iv) を表す

【0087】

【数24】

$$A = (a_{\mu\nu}) \quad \dots (i)$$

$$B = (b_{\mu\nu}) \quad \dots (ii)$$

$$b_{\mu\nu} = c^{a_{\mu\nu}} \quad \dots (iii)$$

$$b_{\mu\nu} = a_{\mu\nu}^c \quad \dots (iv)$$

【0088】

【数 25】

$$g_{0im} = \overrightarrow{g_{i0}}[\overrightarrow{I_{m1}}]$$

$$g_{1im} = \overrightarrow{g_{i1}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{tim} = \overrightarrow{g_{it}}[\overrightarrow{I_{m1}}]$$

$$\vdots$$

$$g_{Tim} = \overrightarrow{g_{iT}}[\overrightarrow{I_{m1}}]$$

$$x_{2im} = \overrightarrow{s_{i2}}[\overrightarrow{I_{m2}}]$$

$$\vdots$$

$$x_{jim} = \overrightarrow{s_{ij}}[\overrightarrow{I_{mj}}]$$

$$\vdots$$

$$x_{kim} = \overrightarrow{s_{iK}}[\overrightarrow{I_{mK}}]$$

$$K_{im} \equiv \prod_{t=0}^T g_{tim}^T C_t y_{im}^{(T-t)}$$

$$\equiv g^{\alpha_i^{-T}} \sum_{t=0}^T C x_{1im}^t y_{im}^{T-t}$$

$$\equiv g^{\alpha_i^{-T}} (x_{1im} + y_{im})^T$$

$$\equiv g^{\alpha_i^{-T}} (x_{1im} + \dots + x_{kim})^T$$

$$\equiv g^{\alpha_i^{-T}} (\alpha_i H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \beta_{i1} + \dots + \alpha_i H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}] + \beta_{iK})^T$$

$$\equiv g^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) + \lambda(N) \}^T$$

$$\equiv g^{\alpha_i^{-T}} \{ \alpha_i (H_1[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}]) \}^T$$

$$\equiv g^{(H_i[\overrightarrow{I_{i1}}][\overrightarrow{I_{m1}}] + \dots + H_K[\overrightarrow{I_{iK}}][\overrightarrow{I_{mK}}])^T} \pmod{N}$$

【0089】

但し、

g_{tim} (=ベクトル g_{it} [ベクトル I_{m1}])

: エンティティ i の特定情報の第 1 ブロックについて自身のベクトル g_{it} から選び出した、エンティティ m のベクトル I_{m1} に対応する成分 ($t = 0, 1, 2, \dots, T$)

$x_{1im} =$ ベクトル s_{i1} [ベクトル I_{m1}]

x_{jim} (=ベクトル s_{ij} [ベクトル I_{mj}])

: エンティティ i の特定情報の第 j ブロックについて自身のベクトル s_{ij} から選び出した、エンティティ m のベクトル I_{mj} に対応する成分 ($j = 2, 3, \dots, K$)

K_{im} : 一方のエンティティ i が他方のエンティティ m に対して生成する共通鍵

y_{im} : ($K - 1$) 個の x_{jim} の和 ($j = 2, 3, \dots, K$)

即ち、 $y_{im} = x_{2im} + x_{3im} + \dots + x_{Kim}$

【図面の簡単な説明】

【図 1】

本発明の暗号通信システムの構成を示す模式図である。

【図 2】

エンティティの ID ベクトルの分割例を示す模式図である。

【図 3】

2 人のエンティティ間における情報の通信状態を示す模式図である。

【図 4】

記録媒体の実施の形態の構成を示す図である。

【符号の説明】

1 センタ

1 a 秘密鍵生成器

1 0, 2 0 メモリ

1 1, 2 1 成分選出器

1 2, 2 2 共通鍵生成器

1 3 暗号化器

2 3 復号器

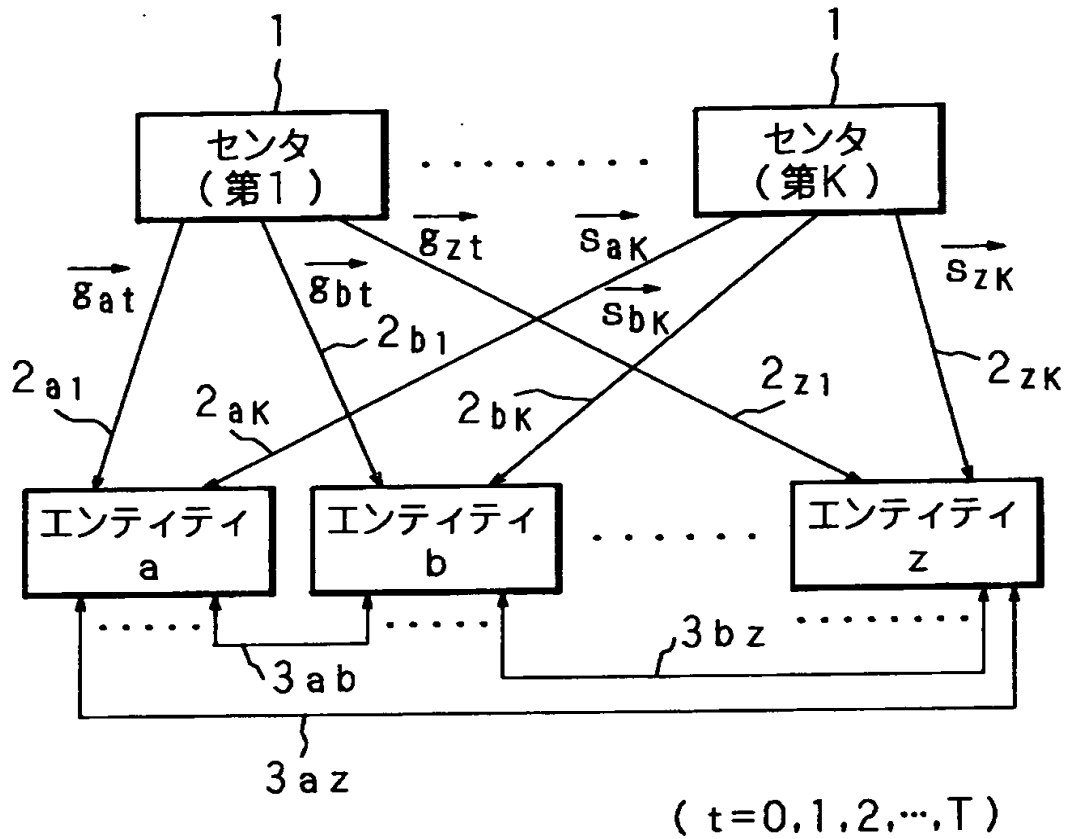
3 0 通信路

4 0 コンピュータ

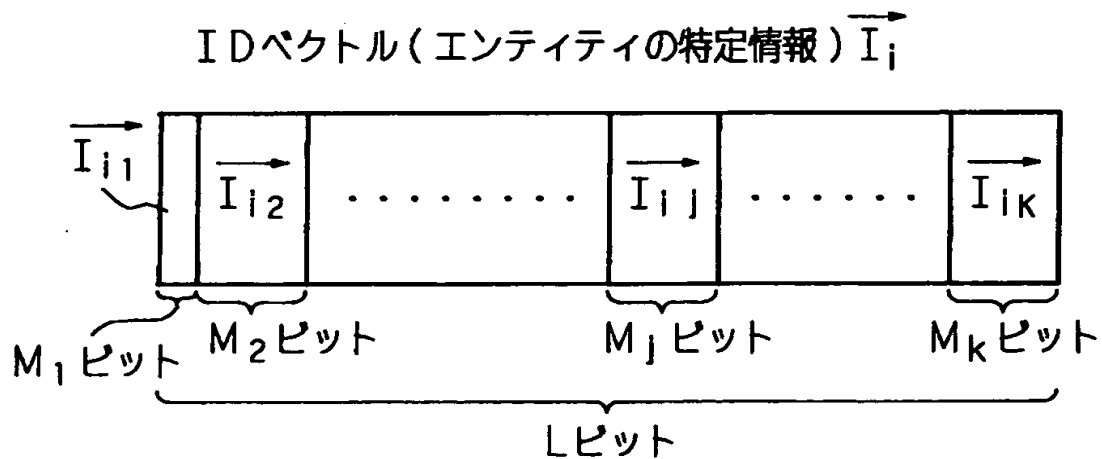
4 1, 4 2, 4 3 記録媒体

【書類名】 図面

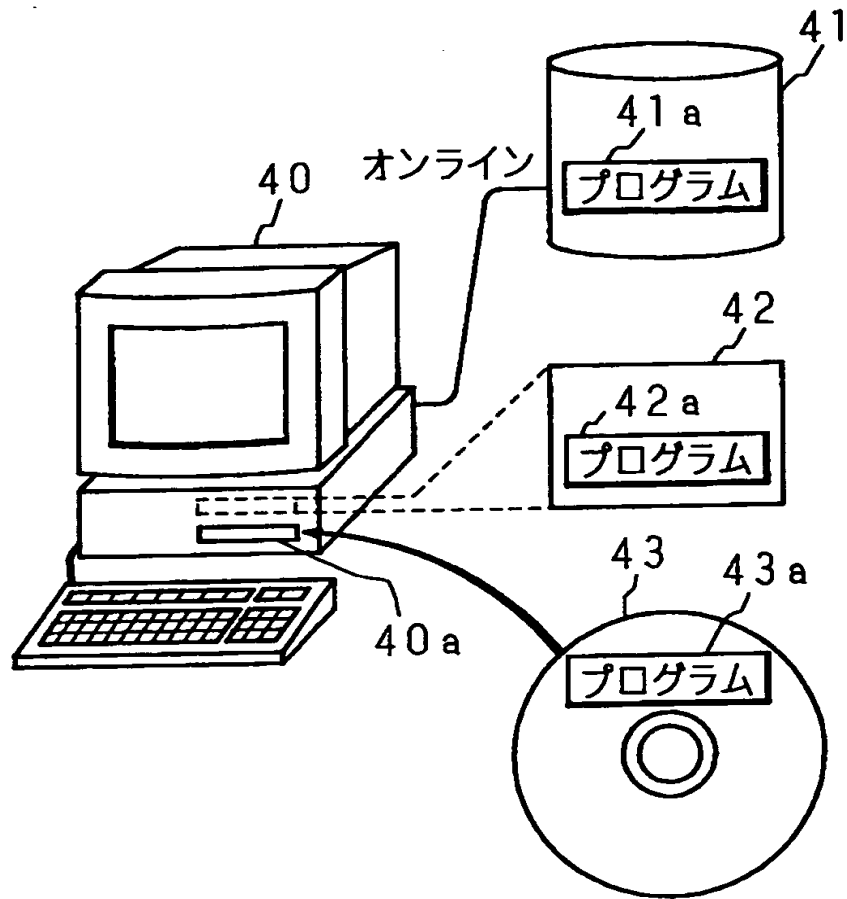
【図 1】



【図 2】



【図 4】



【書類名】 要約書

【要約】

【課題】 結託問題の回避を可能にし、その暗号系の構築が容易である I D－N I K S による暗号通信方法を提供する。

【解決手段】 各エンティティへ固有の秘密鍵を配布するセンタ 1 が複数設けられており、各エンティティの特定情報（I D 情報）をいくつかに分割し、その分割した特定情報毎に作成したすべての秘密鍵をエンティティに配布する。各エンティティは、自身固有の秘密鍵に含まれている、相手のエンティティの分割特定情報に対応する成分を使用して共通鍵を生成する。

【選択図】 図 1

認定・付加情報

特許出願の番号	平成11年 特許願 第059049号
受付番号	59900203160
書類名	特許願
担当官	塩崎 博子 1606
作成日	平成11年 3月16日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000006297
【住所又は居所】	京都府京都市南区吉祥院南落合町3番地
【氏名又は名称】	村田機械株式会社

【特許出願人】

【識別番号】	598159964
【住所又は居所】	東京都渋谷区神宮前四丁目2番19号
【氏名又は名称】	辻井 重男

【特許出願人】

【識別番号】	597008636
【住所又は居所】	大阪府箕面市栗生外院4丁目15番3号
【氏名又は名称】	笠原 正雄

【代理人】

【識別番号】	申請人 100078868
【住所又は居所】	大阪府大阪市中央区釣鐘町二丁目4番3号 河野 特許事務所
【氏名又は名称】	河野 登夫

出 願 人 履 歴 情 報

識別番号 [000006297]

1. 変更年月日 1990年 8月 7日

[変更理由] 新規登録

住 所 京都府京都市南区吉祥院南落合町3番地

氏 名 村田機械株式会社

出 願 人 履 歴 情 報

識別番号 [5 9 7 0 0 8 6 3 6]

1. 変更年月日	1 9 9 7 年 1 月 2 1 日
[変更理由]	新規登録
住 所	大阪府箕面市栗生外院 4 丁目 1 5 番 3 号
氏 名	笠原 正雄

出 願 人 履 歴 情 報

識別番号 [598159964]

1. 変更年月日 1998年11月19日

[変更理由] 新規登録

住 所 東京都渋谷区神宮前四丁目2番19号

氏 名 辻井 重男